UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/784,391	02/15/2001	Kevin C. Jones	EWG-076	3000

23735 7590 11/10/2003

DIGIMARC CORPORATION
19801 SW 72ND AVENUE
SUITE 100
TUALATIN, OR 97062

EXAMINER	
AKHAVANNIK, HUSSEIN	

ART UNIT	PAPER NUMBER
2621	

DATE MAILED: 11/10/2003

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/784,391	JONES, KEVIN C.	
	Examiner	Art Unit	
	Hussein Akhavannik	2621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-12 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-12 is/are rejected.

7)☒ Claim(s) 2 and 7-11 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 15 February 2001 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2,3,8 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

On page 1, line 10 "to" should be deleted.

On page 1, line 14, "internet" should be changed to "Internet".

On page 2, line 10, "guards" should be changed to "guard".

On page 5, lines 1-3, the status of US Patent application Nos. 09/074,034 and 09/127,503 as well as PCT applications PCT/US99/08252 and PCT/US99/14532 should be updated.

On page 7, lines 13-14, all instances of "fag" should be changed to "flag".

Appropriate correction is required.

2. Claims 2 and 7-11 are objected to because of the following informalities:

Referring to claim 2, line 2, "from individual user" should be changed to "from an individual user".

Referring to claim 7, line 1, "data base" should be changed to "database".

Referring to claim 8, line 2, "identify" should be changed to "identity".

Referring to claim 9, line 1, "aparticular" should be changed to "particular".

Referring to claim 9, line 2, "identify" should be changed to "identity".

Referring to claim 9, line 3, "data base" should be changed to "database".

Referring to claim 10, line 5, "data base" should be changed to "database".

Referring to claim 11, line 1, "method specified in claim 10 recited in claim 10" should be changed to "method recited in claim 10".

Appropriate correction is required.

Drawings

3. New corrected drawings are required in this application because the figures are informal. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

4. The drawings are objected to because figure 2 contains a descriptive label. However, figure 2 has already been described in the "Brief Description of the Figures" on page 3 of the specification. The Applicant is advised to change "Fields in a typical watermark payload" to "Watermark Payload" in order to provide a label for the payload illustrated in figure 2. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 4 and 10-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Referring to claim 4, this claim is dependent on claim 4. There is insufficient antecedent basis for this limitation in the claim.

Referring to claim 10, this claim recited "the flags" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Referring to claims 11-12, these claims are indefinite for depending from an indefinite antecedent base claim.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-2 are rejected under 35 U.S.C. 102(e) as being anticipated by Gibbs (U.S. Patent No. 6,615,348).

Referring to claim 1,

i. An electronic messaging system including a mail server which sends and receives messages is illustrated by Gibbs in figure 1 by the authenticated message server (112) and the mail exchanger (108).

ii. The mail server including a watermark reading program which reads watermarks in the messages is explained by Gibbs in column 5, line 47 to column 6, line 33. Gibbs explains that the authenticated message server parses the electronic message to extract a digital signature (corresponding to a digital watermark). Then, Gibbs determines whether an adapted digital signature is present (420 of figure 4) and compares the adapted digital

signature extracted from the message with a newly created adapted digital signature (440 of figure 4).

iii. The mail server controlling the distribution of the messages in response to the data in the watermarks is explained by Gibbs in column 6, lines 33-37. Gibbs explains that if the extracted adapted digital signature does not match with the newly adapted digital signature, then the e-mail message is rejected by the authenticated message server. Referring to claim 2,

i. A means for transmitting messages from an individual user to an e-mail server is illustrated by Gibbs by the connection between the user e-mail client (120) and the mail host (116).

ii. A watermark detecting means for detecting and reading watermarks in e-mail messages before such messages are transmitted from the e-mail server to the Internet is explained by Gibbs in column 5, line 47 to column 6, line 33 and illustrated in figure 1 by the authenticated message server (112). Gibbs explains that the authenticated message server parses the electronic message to extract a digital signature (corresponding to a digital watermark). Then, Gibbs determines whether an adapted digital signature is present (420 of figure 4) and compares the adapted digital signature extracted from the message with a newly created adapted digital signature (440 of figure 4). The processing performed by the authenticated message server (112) is done before the e-mail is transmitted to the Internet as illustrated by Gibbs in figure 1.

iii. A means for preventing the transmission of messages from the e-mail server to the Internet if the watermark detecting means detects a watermark which has an

indication that the message containing the watermark is confidential is explained by Gibbs in column 6, lines 33-37. Gibbs explains that if the extracted adapted digital signature does not match with the newly adapted digital signature, then the e-mail message is rejected (non-authenticated) by the authenticated message server.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al (U.S. Patent No. 5,958,005) in view of Rhoads (U.S. Patent No. 5,862,260).

Referring to claim 1,

i. An electronic messaging system including a mail server which sends and receives messages is illustrated by Thorne et al in figure 1 by the e-mail servers 112 and 114.

ii. The mail server including a watermark reading program which reads watermarks in the messages is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and illustrate the inspecting in figure 5A by reference number 518. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header (as illustrated by Thorne et al in figure 4) as the bodier is embedded within the empirical data steganographically. Thus, by replacing the

header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a mail server include a watermark reading program which reads watermarks in messages in order to determine the flags of a header which has been stored as a watermark (bodier).

iii. The mail server controlling the distribution of the messages in response to the data in the watermarks is explained by Thorne et al in column 7, lines 34-42. The system of Thorne et al will erase or delete an e-mail when the "confidential" flag is raised in the header (which corresponds to a watermark as explained in claim 1ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 2,

i. A means for transmitting messages from an individual user to an e-mail server is illustrated by Thorne et al in figure 1 by the user workstations (118 and 120) connected to an e-mail server (112).

ii. A watermark detecting means for detecting and reading watermarks in e-mail messages before such messages are transmitted from the e-mail server to the Internet is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and

illustrate the inspecting in figure 5A by reference number 518. The email server is explained to be part of the Internet by Thorne et al in column 5, lines 54-67. The mail server reads the header file before the e-mail is transferred to its destination as illustrated by Thorne et al in figure 3. The header is inspected in steps 323 and 324 before it is sent in step 328. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header (as illustrated by Thorne et al in figure 4) as the bodier is embedded within the empirical data steganographically. Thus, by replacing the header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to detect and read watermarks in e-mail messages before such images are transmitted from the server to the Internet in order to determine the flags of a header which has been stored as a watermark (bodier).

iii. A means for preventing the transmission of messages from the e-mail server to the Internet of the watermark detecting means detects a watermark which has an indication that the message containing the watermark is confidential is explained by Thorne et al in column 7, lines 34-42. The system of Thorne et al will erase or delete an e-mail when the "confidential" flag is raised in the header (which corresponds to a watermark as explained in claim 2ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such

as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 3,

i. A system for controlling the distribution of electronic messages that contain confidential information is illustrated by Thorne et al in figure 3.

ii. Each electronic message that contains confidential information including a digital watermark carrying data that indicates that the message is confidential is not explicitly explained by Thorne et al. Thorne et al do illustrate a header that contains a confidentiality field in figure 4. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header as the bodier is embedded within the empirical data steganographically. Thus, by replacing the header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to input a digital watermark carrying data that indicates that an e-mail is confidential in order to categorize the e-mail imperceptibly.

iii. A server which transmits and receives messages is illustrated by Thorne et al in figure 1 by the e-mail servers (112 and 114).

iv. The server including a watermark reading program which reads watermarks in messages and controls the distribution of such messages in accordance with the data carried by any watermarks in the messages is explained by Thorne et al in column 7, lines

34-42. The server of Thorne et al will erase or delete an e-mail when the "confidential" flag is raised in the header (which corresponds to a watermark as explained in claim 3ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 4, the messages being transmitted over the Internet is explained by Thorne et al in column 5, lines 54-67.

Referring to claim 5,

i. Controlling the distribution of electronic messages that contain confidential information is illustrated by Thorne et al in figure 3.

ii. The messages containing digital watermarks which carry data indicating that the message contains confidential information is not explicitly explained by Thorne et al. Thorne et al do illustrate a header that contains a confidentiality field in figure 4. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header as the bodier is embedded within the empirical data steganographically. Thus, by replacing the header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to input a digital watermark

carrying data that indicates that an e-mail is confidential in order to categorize the e-mail imperceptibly.

iii. Reading the watermarks in messages prior to transmission of the messages is illustrated by Thorne et al in figure 3. The mail server reads the header file (steps 323 and 324) before the e-mail is transferred to its destination (sending of step 328).

iv. Controlling the distribution of each electronic message which contains a watermark in response to the data carried by the watermark in the message is explained by Thorne et al in column 7, lines 34-42. The server of Thorne et al will erase or delete an e-mail when the "confidential" flag is raised in the header (which corresponds to a watermark as explained in claim 5ii), thereby ending the distribution of the e-mail. Furthermore, additional flags in the header also control the distribution of the e-mail such as the forward flag which either permits or prohibits the forwarding of an e-mail as explained by Thorne et al in column 7, line 66 to column 8, line 12.

Referring to claim 6, the messages being transmitted over the Internet corresponds to claim 4.

11. Claims 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thorne et al in view of Rhoads as applied to claims 1-6 above, and further in view of Kasiraj et al (EP Patent Application Pub. No. 0,375,138).

Referring to claim 7, a database being interrogated to determine the action to take with a particular message is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. Such interrogation is performed to control

distribution of electronic messages to recipients which meet certain criteria. By interrogating the database of Kasiraj et al when the confidential flag of Thorne et al and Rhoads is raised, the security of the e-mail server of Thorne et al and Rhoads would be improved. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to interrogate a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 8, the action taken with respect to a particular message is dependent of the identity of the sender, the identity of the receiver, and information carried by the watermark is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. The profile is explained to include the recipient's security classification, the identifying information of the source (sender) and the content of the e-mail (which will include the bodier of the system of Thorne et al and Rhoads). By using the identity of the sender, the identity of the receiver, and information carried by the watermark, a database can be interrogated to control distribution of electronic messages to recipients which meet certain criteria. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the identity of the sender, the identity of the receiver, and information carried by the watermark when interrogating a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 9, the action taken with respect to a particular message being dependent on the identity of the sender, the identity of the receiver, information carried by the

watermark, and information stored in a database is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. The profile is further explained to include the recipient's security classification, the identifying information of the source (sender) and the content of the e-mail (which will include the bodier of the system of Thorne et al and Rhoads). By using the identity of the sender, the identity of the receiver, and information carried by the watermark, a database can be interrogated to control distribution of electronic messages to recipients which meet certain criteria. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the identity of the sender, the identity of the receiver, and information carried by the watermark when interrogating a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 10,

i. Detecting and reading digital watermarks contained in such messages to determine how the flags in such watermarks are set is not explicitly explained by Thorne et al. Thorne et al do explain inspecting the header of an e-mail in order to determine whether the e-mail is secure in column 9, lines 54-59 and illustrate the inspecting in figure 5A by reference number 518. Thorne et al also explain that the field of the header correspond to flags in column 8, lines 28-42. Rhoads explains that a "bodier" can be used to replace a header in column 41, lines 20-40. By using such a bodier, the header cannot be simply stripped off in an attempt to remove the confidential flag in a header (as

illustrated by Thorne et al in figure 4) as the bodier is embedded within the empirical data steganographically. Thus, by replacing the header of Thorne et al by the bodier as explained by Rhoads, the security of the imperceptibility and robustness of the header information would be increased. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a mail server include a watermark reading program which reads watermarks in messages in order to determine the flags of a header which has been stored as a watermark (bodier).

ii. Interrogating a database to determine what action should be taken with a message based upon the identity of the sender, the identity of the receiver and the flag setting in the watermark in the message is not explicitly explained by Thorne et al or Rhoads. However, Kasiraj et al do explain comparing an electronic message profile with a previously established profile (inherently contained in a database) in the abstract. The profile is further explained to include the recipient's security classification, the identifying information of the source (sender) and the content of the e-mail (which will include the bodier of the system of Thorne et al and Rhoads). By using the identity of the sender, the identity of the receiver, and information carried by the watermark, a database can be interrogated to control distribution of electronic messages to recipients which meet certain criteria. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the identity of the sender, the identity of the receiver, and information carried by the watermark when interrogating a database to determine the action to take (send or not send) with a particular message in order to improve the security of e-mail distribution in the network of Thorne et al and Rhoads.

Referring to claim 11,the messages being transmitted over the internet corresponds to claim 4.

Referring to claim 12, the data carried by the watermark indicating if the message contains confidential information is illustrated by Thorne et al in figure 4 by the confidential field of the header, which is used to create the bodier (corresponding to claim 10i).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nakamura et al (Japanese Patent App. Pub. No. 2003-092605) – To exhibit illegal distribution of electronic mail in an electronic mail server by embedding an electronic watermark as explained in the abstract.

Kujirada (Japanese Patent App. Pub. No. 2000-057327) – To exhibit an electronic watermark explaining the image information to control electronic information supply as explained in the abstract.

Beyda (European Patent App. Pub. No. EP 1193925 A2) – To exhibit an electronic message server which prevents intentional and unintentional transmission of electronic messages as explained in the abstract.

Brown et al (U.S. Patent App. Pub. No. 2003/00236852) – To exhibit traceable message entries using electronic watermarks as explained in the abstract.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hussein Akhavannik whose telephone number is (703)306-4049. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo H. Boudreau can be reached on (703)305-4706. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

Hussein Akhavannik H.A.
October 31, 2003

LEO BOUDREAU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600